Amendments to the Claims:

Please cancel claim 1 presented in the underlying International Application No. PCT/DE2004/001252 without prejudice, and add new claims 2-16 as shown in the listing of claims.

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (canceled)

Claim 2 (new): A method for data storage on a server in a telecommunications network, the telecommunications network providing connectivity between local computers of users and the server, the method comprising:

upon request, issuing, by an operator of the server, to a first user of the users a user certificate for access conditions, and providing the user certificate and a secret key to the first user;

accessing the server over an internet;

sending, by the server, a client program to a first local computer of the first user, the client program enabling an authentication of the first user using the user certificate and a transmission of at least one further security requirement; and

setting up a personal main folder on the server for the first user, the main folder having a first file including a first security requirement defined for the main folder and first management information so as to provide a main locker, the main folder being configured to have at least one further folder set up therein, the at least one further folder having a function and a second file including a second security requirement defined for the at least one further folder and including second management information so as to provide a functional locker, the functional locker being

displayed only if at least one security-relevant requirement is met so as to provide a locker system having a virtual character, the functional locker providing a function of at least one of:

a personal locker, first files being storable in the personal locker only by the first user and displayable only to the first user;

a provisioning locker, a first reference to a second file for another user being storable by the first user therein;

a receiving locker for a third file of a sender user of the users, the receiving locker being configured, when opened, to provide to the first user a sender user reference relating to the storage of the third file and to a sender user defined security requirement; and

a public locker configured to store, by the first user, the first reference to the second file when the first reference is stored in the provisioning locker, which, when the first reference is intended for a plurality of other users.

Claim 3 (new): The method as recited in claim 2 wherein the certificate includes a public key.

Claim 4 (new): The method as recited in claim 2 further comprising providing a public key to the first user.

Claim 5 (new): The method as recited in claim 2 wherein the providing the user certificate and a secret key to the first user is performed by providing the user certificate and a secret key on a smart card.

Claim 6 (new): The method as recited in claim 2 wherein the at least one further security requirement includes at least one of a biometric system requirement, a geographic positioning requirement, a time restriction, a network requirement, and a computer data requirement.

Claim 7 (new): The method as recited in claim 6 wherein the at least one further security requirement includes a time dependency.

Claim 8 (new): The method as recited in claim 2 wherein the at least one security-relevant requirement is a requirement of the operator of the server, the first user, and the sender of the third file.

Claim 9 (new): The method as recited in claim 2 wherein the provisioning locker has a name associated therewith.

Claim 10 (new): The method as recited in claim 2 wherein the provisioning locker includes a user locker for the another user.

Claim 11 (new): The method as recited in claim 2 wherein the receiving locker has a name associated with the sender of the third file.

Claim 12 (new): The method as recited in claim 2 wherein the receiving locker includes a user locker for the sender user.

Claim 13 (new): The method as recited in claim 2 wherein the first user is a user registered with the server, and further comprising setting up a second personal main folder on the server for a second user registered with the server, the second main folder having a respective first file including a respective first security requirement defined for the respective main folder and respective management information so as to provide a respective locker, each respective main folder being configured to have respective further folders set up therein, the respective further folders each having a respective function and each having a respective second file including a respective second security requirement defined for the respective further folder and including respective management information, each of the further folders acting as a respective functional

locker, each functional locker being displayed only if a respective security-relevant requirement is met, so as to provide a respective locker system having a virtual character, each functional locker providing a respective function of at least one of:

a respective personal locker, respective first files being storable in the personal locker only by the respective user and displayable only to the respective user;

a respective provisioning locker, a respective first reference to a respective second file for another user being storable by the respective user therein;

a respective receiving locker for a respective third file of a respective sender user of the users, the respective receiving locker being configured, when opened, to provide to the respective user a respective sender user reference relating to the storage of the respective third file and to a respective sender user defined security requirement; and

a respective public locker configured to store, by the first user, the first reference to the second file when the first reference is stored in the provisioning locker, which, when the first reference is intended for a plurality of other users.

Claim 14 (new): The method as recited in claim 2 further comprising:

storing a fourth file in the functional locker only if the second security requirement is met;

generating a random number from data of the fourth file so as to provide an access key;

encrypting the data using the access key;

subsequently encrypting the access key with the public key and then destroying the access key so that the access key, for accessing the stored file, can only be recovered using the secret key;

transmitting, to the server, the encrypted data, fourth management information of the fourth file, and the encrypted access key;

encrypting, by the server, the transmitted encrypted data a second time;

generating a unique file identifier for the fourth file;

storing the fourth file in a system locker using the file identifier; and

storing a fourth reference to the fourth file in the functional locker, the fourth reference including the file identifier, the encrypted access key, and the fourth management information.

Claim 15 (new): The method as recited in claim 14 wherein the functional locker is a provisioning locker including a user file for the another user, and further comprising enabling the stored fourth file to be forwarded by the first user to the another user only if the first user decrypts the encrypted access key with the secret key and re-encrypts the decrypted access key with a second public key of the another user, and the re-encrypted access key, the file identifier and the fourth management information, are stored as the fourth reference to the file into the user locker.

Claim 16 (new): The method as recited in claim 1 wherein the second management information includes a management requirement, and wherein the storing the fourth file is performed only if the management requirement is met.